REMARKS/ARGUMENTS

The Examiner objects to Claims 3, 9, 11-12, 23, 33-34, 39, 43, and 52-53 based on various informalities. Applicant has amended claims 3, 9, 11, and 12 to overcome the objections. The remaining claims have been canceled.

The Examiner rejects Claim 43 under 35 U.S.C.§112, second paragraph. This rejection is moot in light of the cancellation of Claim 43.

The Examiner rejects Claims 1, 4-5, 12-15, 17-20, 21-24, 26-27, 35-37, 40-44, 46, and 54-62 under 35 U.S.C.§102(b) as being anticipated by Menon, et al. (U.S. 2001/0001268); and Claims 2, 25, and 45 under 35 U.S.C.§103(a) as being unpatentable over Menon, et al., and further in view of Chan, et al. (U.S. 6,128,389); Claims 3, 34, and 53 in view of Menon, et al., and further in view of Rai, et al. (U.S. 6,675,208); Claims 6, 8, 28, 30, 39, 47, and 49 in view of Menon, et al. And further in view of Molva, et al. (U.S. 5,347,580); Claims 7, 29, and 48 in view of Menon, et al., and further in view of Chan, et al. (U.S. 6,128,389); Claims 9, 31, and 50 in view of Menon, et al., and further in view of Kochker, et al.(U.S. 20020099948); Claims 10, 32, and 51 in view of Menon, et al., and further in view of Chan, et al.; Claims 11, 33, and 52 in view of Menon, et al., and further in view of Boate, et al. (U.S. 20020104006); and Claims 16 and 38 in view of Menon, et al., and further in view of Chan, et al.

The cited references fail to teach or suggest at least the following italicized features of the amended and newly added independent claims:

> 1. A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:
>
> (a) providing an unprovisioned first packet-switched communications device in an enterprise network, the first packet-switched communications device having a corresponding unique identifier and an electronic address on the enterprise network;
>
> (b) *as part of the provisioning process establishing, by the first packet-switched communications device, a secure communications session with a key generating agent in the enterprise network*;
>
> (c) providing, to the key generating agent through the session, (i) when a key *identifier is derived using the unique identifier associated with the first packet-switched communications device, the unique identifier or (ii) when the key*

identifier is derived using information not associated with the first packet-switched communications device, no unique identifier;

(d) *receiving, from the key generating agent through the session, (i) a secret key derived from an enterprise master key and a key identifier and (ii) the key identifier*;

(e) *forwarding to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first packet-switched communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first packet-switched communications device is successfully registered in step (g)*;

(f) *authenticating the first packet-switched communications device with the secret key or an authentication key derived therefrom*; and

(g) *when the first packet-switched communications device is successfully authenticated, registering the first packet-switched communications device, wherein steps (b) through (e) occur after the first packet-switched communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.*

63. An enterprise network including a first packet-switched communications device having a corresponding unique identifier and an electronic address on the enterprise network, the first packet-switched communications device comprising: a first processor in the packet-switched communications device operable to:

(A1) *establish, as part of a provisioning process, a secure communications session with a key generating agent in the enterprise network*;

(A2) *provide, to the key generating agent through the session, (i) when a key identifier is derived using a unique identifier associated with the first packet-switched communications device, the unique identifier or (ii) when the key identifier is derived using information not associated with the first packet-switched communications device, no unique identifier*;

(A3) *receive, from the key generating agent through the session, (i) a secret key derived from a key identifier and an enterprise master key and (ii) the key identifier*;

(A4) *forward to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first packet-switched communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first packet-switched communications device is successfully registered in operation (B2)*; and wherein the application server comprises a second processor that is operable to:

(B1) *authenticate the communications device with the secret key or an authentication key derived therefrom*; and

(B2) *when the communications device is successfully authenticated, register the communications device, wherein operations (A1) through (B1) occur after the first packet-switched communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.*

82. A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:
(a) assigning an electronic address to a first communications device;
(b) providing the electronic address and an address associated with a key generating agent to the first communications device;
(c) authenticating, by the first communications device, the key generating agent; and
(d) when authentication of the key generating agent is successful, performing the following additional steps:
(e) *establishing, as part of the provisioning process, a secure communications session between the first communications device and the key generating agent, wherein the first communications device has a corresponding unique identifier*;
(f) *providing the unique identifier to the key generating agent through the secure communications session*;
(g) *receiving, from the key generating agent through the session, (i) a secret key derived from an enterprise master key, the unique identifier, and a key identifier and (ii) the key identifier*;
(h) *forwarding to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first communications device is successfully registered in step (j)*;
(i) *authenticating the first communications device with the secret key or an authentication key derived therefrom*; and
(j) *when the first communications device is successfully authenticated, registering the first communications device, wherein steps (e) through (j) occur after the first communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.*

U.S. 2001/0001268 to Menon, et al.

Menon, et al., are directed to a telecommunications network supporting wireless access to one or more public packet data networks, including, but not limited to, the Internet, and to one or more public switched circuit networks, for example, but not limited to, the Public Switched Telephone Network (PSTN). A voice access unit, for example, a telephone, may be connected to a Customer Premise Radio Unit (CPRU) via a wireline interface. The CPRU provides the voice access unit over-the-air, i.e., radio, access to one or more public switched circuit networks. A computing device, for example, a personal computer, may also, or in the alternative, be connected to a CPRU via a wireline interface. The CPRU provides the personal computer over-the-air access to one or more public packet data networks. A facsimile device may also, or in the alternative, be connected to a CPRU via a wireline interface. The CPRU provides the facsimile device over-the-air access to one or more public switched circuit networks. The telecommunications network comprises a base station which provides wireless access for CPRUs to one or more public packet data networks and/or public switched circuit networks. The telecommunications network further comprises a Wireless Adjunct InteRnet Platform (WARP), which supports functionality of known base stations. The telecommunications network also comprises one or more access routers, H.323 gateways, H.323 gatekeepers, Internet gateways and fax gateways for supporting subscriber access to public packet data networks and public switched circuit networks.

Menon, et al., does not teach the phone 15 having a secret key to protect communications between the phone 15 and other components 12, 20, and 25 in the premises or LAN. The CPRU 25 is the only component in the premises network having a secret key for communications over the wireless WAN.

Menon, et al., require prior knowledge of the secret key. In ¶[01750], Menon, et al., state:

> The CPRU 170 automatically initiates the terminal authentication process upon power on. In an embodiment, the CPRU 170 communicates with the respective WARP 174 for terminal authentication via the Terminal Management Protocol (TMP). *The CPRU 170 has a secret key installed in the factory; the secret key is*

> *associated with the CPRU's unique universal identifier*. The CPRU 170 also comprises dedicated circuitry and/or software to compute responses to given terminal authentication challenges issued by the Subscriber Management Platform (SMP), using its secret key.

(Emphasis supplied.)

These deficiencies are not overcome by the remaining references.

U.S. 6,128,389 to Chan, et al.

Chan, et al., are directed to a system and method for enabling sensitive authentication information to be under the control of the service provider and transmitting only non-sensitive authentication information to the AC, and for providing a secure technique for generating sensitive authentication information and for securely transmitting to and storing the information in the mobile system (MS) and a storage device controlled by the service provider. Chan, et al., utilize a secure authentication center (SAC) and a secure A-key management system (SAMS) to perform authentication. Chan, et al., automatically and securely generate and program an MS and SAMS with the sensitive authentication information while significantly reducing the risk of misappropriation of the sensitive authentication information. The risk of misappropriation is reduced since the sensitive authentication information (or other sensitive information) need not be pre-programmed into the MS, or if it is pre-programmed, the sensitive authentication information can be re-programmed, thereby reducing the potential access to the information by unauthorized people before the MS is sold. In addition, the risk of misappropriation is reduced since the generation and programming system and method is performed automatically using a secured communication technique.

U.S. 6,675,208 to Rai, et al.

Rai, et al., are directed to a coupled data network with a system for registering end systems. A foreign network includes a foreign mobile switching center and a foreign base station. The foreign mobile switching center includes a serving registration server, the foreign base station includes a foreign access hub, and the foreign access hub includes a proxy registration

agent. A home network includes a home mobile switching center with a home registration server. A first end system subscribes to the home network and operates within the foreign network. The end system includes an end registration agent, the end registration agent being coupled to the proxy registration agent, the proxy registration agent being coupled to the serving registration server, and the serving registration server being coupled to the home registration server.

U.S. 5,347,580 to Molva, et al.

Molva, et al., are directed to a novel smartcard-based authentication technique using a smartcard that encrypts the time displayed on the card with a secret, cryptographically strong key. The (public) work station receives as input certain values defining the user, the card and a particular value derived from the encrypted time and encrypts and/or transmits these values to the server. The server, in turn, computes from received values some potential values and compares these to other received values. If the server determines a match, an accept signal is transmitted to the work station.

U.S. 2002/0099948 to Kocher, et al.

Kocher, et al., requires, before use, a population of tamper-resistant cryptographic enforcement devices partitioned into groups and the issuance of one or more group keys. Each tamper-resistant device contains multiple computational units to control access to digital content. One of the computational units within each tamper-resistant device communicates with another of the computational units acting as an interface control processor, and serves to protect the contents of a nonvolatile memory from unauthorized access or modification by other portions of the tamper-resistant device, while performing cryptographic computations using the memory contents. Content providers enforce viewing privileges by transmitting encrypted rights keys to a large number of recipient devices. These recipient devices process received messages using the protected processing environment and memory space of the secure unit. The processing result depends on whether the recipient device was specified by the content provider as authorized to view some encrypted digital content. Authorized recipient devices can use the processing result

in decrypting the content, while unauthorized devices cannot decrypt the content. A related aspect of the invention provides for securing computational units and controlling attacks. For example, updates to the nonvolatile memory, including program updates, are supported and protected via a cryptographic unlocking and validation process in the secure unit, which can include digital signature verification.

U.S. 2002/0104006 to Boate, et al.

Boate, et al., are directed to an improved computer network security system and method, and a personal identifier device used for controlling network access, to provide real time authentication of both a person's identity and presence at a computer workstation. A new user is registered to a portable personal digital identifier device and, within the portable personal digital identifier device, an input biometric of the user is received and a master template is derived therefrom and securely maintained in storage. A private key is also generated and securely maintained in the storage and a public key corresponding to the private key is generated and provided for external storage (in the network). A public key corresponding to a private key associated with a network security manager component is also stored in the device storage. When the personal digital identifier device is within an envelope area proximate the workstation a first signal is transmitted from a base unit associated with the workstation to the personal digital identifier device and the personal digital identifier device automatically transmits a response signal establishing communications between the base unit and the personal digital identifier device. The personal digital identifier device verifies the origin of a digitally signed challenge message from the network security manager component. A digitally and biometrically signed challenge response message is produced and transmitted by the personal digital identifier device in response to the verified challenge message. An image of the user may be displayed on the workstation screen when the user's personal digital identifier device is located within the envelope.

Accordingly, the pending claims are allowable.

The dependent claims provide further reasons for allowance.

By way of example, dependent claim 2 requires the key identifier to be a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function and the secret key not to be in the possession of the first packet-switched communications device before step (d).

Dependent claim 3 requires the electronic address to be a telephone extension, the first packet-switched communications device to possess the secret key, the first packet-switched communications device not to be in secure communications with the application server, and the first packet-switched communications device to provide the registration request to the application server using the key identifier.

Dependent claim 4 further includes before the establishing step:

authenticating the key generating agent;

performing the establishing, providing, and receiving steps when authenticating the key generating agent is successful.

Dependent claim 5 requires the secret key to be a symmetric key and the authentication step (f) to be performed using symmetric key cryptography.

Dependent claim 6 requires the secret key to be derived from the enterprise master key, the key identifier, and at least one of an attribute associated with the key generating agent and the unique identifier.

Dependent claim 7 requires the enterprise master key to be calculated using a seed value and a pseudorandom number generator, the secret key to be derived using the key generating agent attribute and unique identifier, the attribute of key generating agent to be an electronic address of the key generating agent and/or an electronic address of a server the key generating agent is resident on, and the unique identifier to be the address of the first packet-switched communications device and/or a serial number associated with the first packet-switched

communications device.

Dependent claim 8 requires the authentication key to be used in authenticating step (f), an integrity check value used in step (f) to be a hashed message authentication code using the secret key, and the authentication key to be derived from the secret key of the first packet-switched communications device and an attribute of the first packet-switched communications device.

Dependent claim 9 requires the key identifier computed from the unique identifier to comprise at least a first field, the first field comprising an identifier associated with the key generating agent, a second field comprising the identifier of the first packet-switched communications device, and a counter field.

Dependent claim 10 requires the unique identifier of the first packet-switched communications device to be at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the first packet-switched communications device on the enterprise network.

Dependent claim 11 further requires the step:

digitally signing a message, wherein a digital signature is derived from the secret key, a constant, and a personal identification number of a user associated with the first packet-switched communications device.

Dependent claim 12 requires a session pre-master secret to be used, after step (g), by the first packet-switched communications device for establishing a secured session and the pre-master secret to be a function of the secret key, the unique identifier, a nonce value.

Dependent claim 13 requires the establishing step (b) to comprise the sub-steps:

(B1) receiving a first IP address assigned to the first packet-switched communications device and a second IP address assigned to an enterprise server comprising the key generating agent;

(B2) the first packet-switched communications device authenticating the enterprise server

using public cryptography techniques;

(B3) the first packet-switched communications device generating a second secret key;

(B4) the first packet-switched communications device encrypting the second secret key with a public key associated with the enterprise server; and

(B5) the first packet-switched communications device sending the encrypted second secret key to the enterprise server.

Dependent claim 14 requires the establishing step to include the sub-steps:

establishing a logical connection with the key generating agent;

negotiating security parameters;

authenticating the identity of the key generating agent; and

when authentication is successful, activating the negotiated security parameters to establish the secured communications session.

Dependent claim 15 requires the additional step:

when authentication is successful, establishing secure communications.

Dependent claim 16 requires the providing step to comprise prompting a user associated with the first packet-switched communications device for a personal identification number and unique identifier.

Dependent claim 17 requires the first packet-switched communications device to provide to the key generating agent through the session, the key identifier when the first packet-switched communications device computes the key identifier.

Dependent claim 18 further requires the steps:

closing the secured session; and

computing a packet switched device authentication key using the secret key.

Dependent claim 19 requires the step of authenticating to further include:

when authentication is successful, establishing secure communication with the first packet-switched communications device.

The newly added dependent claims provide additional distinctions over the cited references.

Based upon the foregoing, Applicants believe that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,
SHERIDAN ROSS P.C.

By: Douglas Swartz

Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: August 30, 2007